WORKSHOP:

Principles in Secure Mobile Application Development

Mobile applications and web services have become an essential element of enterprise solutions. Many companies provide their web services to end users with mobile platforms, devices and services. Unfortunately mobile platforms and web services have many security weaknesses. Compatibility for different mobile platforms, weak integration of platform security technologies, insufficient protection of private information and insecure corporate service access are major concerns. Because of these business risks, secure mobile application and web service design, development and testing procedures should be used by business managers, software developers, auditors and security engineers.

Unlike other courses, our workshop not only provides a foundational understanding of secure coding techniques, but it also provides a practical attack-demonstration. Your team will get to see first-hand how practical attacks are masterminded, and see the common tools used to carry them out.

A Sense of Security ethical hacker will prepare in advance a custom attack demonstration highly-relevant to your team. Witnessing the real-world tactics, techniques, and procedures used by an attacker is an eye-opener, and a game changer for your team.

KEY BENEFITS

- **Understand your attacker** – see first-hand the tools and tactics likely to be used by real-world attackers to find vulnerabilities in your mobile application.
- **Increase development efficiency** – learn how to prevent software engineering defects as early as possible, avoiding unnecessary re-work and endless bug tickets.
- **Boost application quality** – discover how mobile application security testing works, and understand the value in unit testing and other software testing practices.
- **Improve platform security** - invite your operations team who may also benefit from understanding the attack vectors, and secure their environment configurations.
- **Quick Reference Guide** – each attendee receives their own laminated security quick reference guide, outlining core areas of focus with checklists.
- **Ask the Experts** – our workshops incorporate dedicated question & answer time so your team can address nagging questions that make the biggest difference.

WHO CONDUCTS THE TRAINING?

Your assigned trainer/instructor will be a senior member of Sense of Security's Research and Technical Assurance Practice. Our Trainers possess an advanced knowledge of mobile application security from diverse backgrounds and are actively involved in the application, wireless and mobile security community.

WHO SHOULD ATTEND THIS WORKSHOP?

The Principles in Secure Mobile Application Development workshop has been designed for software developers and engineers and contains advanced technical concepts.

We recommend also inviting operations team leads, or network and system administrators, as they'll see the bigger picture, and learn how to better secure your web infrastructure.

HOW IS THIS WORKSHOP DELIVERED?

This workshop is provided as instructor led content at your office, or a venue of your choosing. Each workshop is limited to a maximum of 10 attendees and is conducted over one full day. Other arrangements can be made by prior agreement.

Sense of Security®

WHAT INFORMATION DOES THIS WORKSHOP INCLUDE?

The workshop includes best practice mobile application security development methodologies relevant to both leading mobile platforms. We discuss your requirements beforehand, and include language specific examples relevant to your environment, and devise an attack demonstration. The training will cover Android , iOS and cross platform development (Xamarin).

Our continual research and development of this workshop includes best practice security including OWASP Mobile Top 10. As a PCI QSA company, Sense of Security also ensures that PCI compliance requirements are met.

The workshop covers the following topics which will be delivered across an Introductory and an Advanced Module.

Development Options

- Toolchains
- Compilation
- Cross Platform Development
- Native and High-Level Code
- Target Platform Security

Device Management

- Root Detection
- Anti-Tampering

Secure Storage

- Encryption Issues
- Keystore/Keychain
- File System Hierarchy

Other

- Caching
- Secure Logging
- Obfuscation
- Permission Usage
- 3rd Party Libraries
- Sandboxing
- Designing Secure UI's
- Embedding secure processes in the SDLC

WHY CHOOSE SENSE OF SECURITY?

Security is our core business — it's all we do. Sense of Security has 15+ years of extensive knowledge of the technical, commercial, and regulatory aspects of IT security.

Experience and focus — our consultants are experienced security specialists with a business focus, creating security solutions that mitigate risk and maximise results.

Trusted advisors — major names in the Banking & Finance, Insurance, Healthcare, Retail, Service Provider sectors as well as Resources, Utilities & Telecommunications rely on Sense of Security. We also conduct business with Local, State and Federal governments.

Authentication / Authorisation

- Password Based
- SSO
- Oauth
- Mutual SSL/TLS Authentication

Networking and Transport Layer

- Mutual SSL/TLS Authentication
- Private APNs
- SSL/TLS Configuration and Management
- Certificate Pinning
- HTTP Proxy

Hardware Integrations

- On Device Subsystems
- External / Third Party Devices
- Peer-to-Peer communications

SECURITY OPERATIONAL TECHNICAL SPECIALISED

Sense of Security®

SYDNEY
Level 8, 66 King St, Sydney, NSW 2000

MELBOURNE
Level 15, 401 Docklands Dr, Docklands, VIC 3008

CONTACT US TODAY
1300 922 923

info@senseofsecurity.com.au